(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－187826

(43)公開日　平成10年(1998)７月21日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　17/60		Ｇ０６Ｆ　15/21	３４０Ｃ
19/00		Ｇ０６Ｋ　17/00	Ｓ
Ｇ０６Ｋ　17/00		Ｇ０７Ｄ　9/00	４６１Ｚ
Ｇ０７Ｄ　9/00	４６１	Ｇ０６Ｆ　15/30	３３０
Ｇ０７Ｆ　7/12		Ｇ０７Ｆ　7/08	Ｃ

審査請求　有　請求項の数５　ＦＤ　（全 13 頁）

(21)出願番号　特願平8－354467

(22)出願日　平成８年(1996)12月19日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　島田　道雄
東京都港区芝五丁目７番１号　日本電気株式会社内

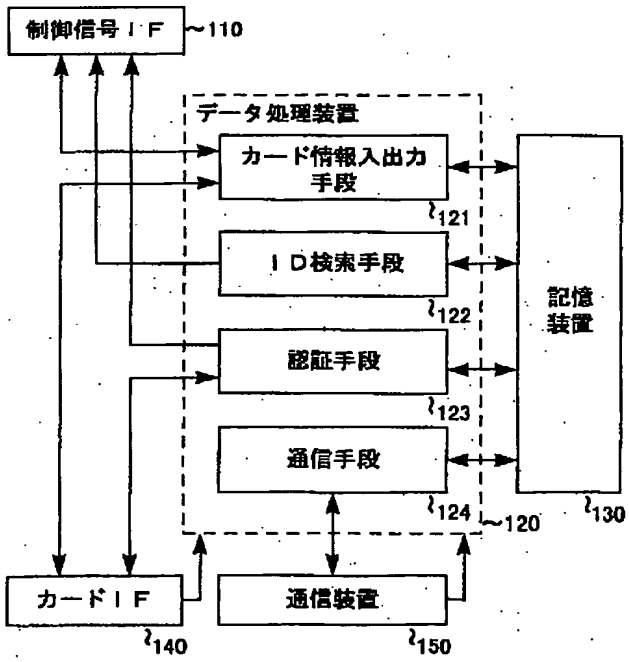
(74)代理人　弁理士　境　廣巳

(54)【発明の名称】　偽造カード使用防止方法およびカード読取書込装置ならびに偽造カード使用防止システム

(57)【要約】

【課題】　センタ装置とリアルタイムで通信しないで、また、カード内部で高度な暗号化を行わないで、偽造カードの使用を困難にする。

【解決手段】　ＩＣカードの使用時、カード読取書込装置のＩＤ検索手段１２２は、カードのＩＤが記憶装置１３０に記憶されているブラックリストに登録されているか否かを調べ、登録されていれば偽造カードであると判定する。また、認証手段１２３は、カードと通信を行ってカードを認証し、もし、カードが認証されなかったら、偽造カードであると判定する。通信手段１２４は、センタ装置と非リアルタイムで通信し、センタ装置にカード情報を送信するとともに、センタ装置からブラックリストに追加するＩＤを受信する。



【特許請求の範囲】

【請求項１】　カードの不正な使用を防止する方法において、

カード読取書込装置によってカードから取得したＩＤや使用履歴などのカード情報を非リアルタイムにセンタ装置に送信し、センタ装置においてカードの使用履歴の推移を評価して論理的な矛盾を含むカードのＩＤをブラックＩＤとして検出してカード読取書込装置に送信することで、カード読取書込装置の保持するブラックリストを逐次更新し、

カードの使用時は、カード読取書込装置において、そのカードのＩＤとブラックリスト中のＩＤとの比較によって不正なカードを検出すると共に、更に、カードとの通信によってそのカードが正規のものか否かを識別する認証を行うことを特徴とする偽造カード使用防止方法。

【請求項２】　カードの不正な使用を防止する機能を有するカード読取書込装置であって、

カードの使用者に対してサービスを提供する外部装置との通信を行うための制御信号インタフェースと、

カードとの通信を行うためのカードインタフェースと、

センタ装置との通信を行うための通信装置と、

前記センタ装置から送られてきた偽造カードにかかるＩＤを登録してあるブラックリストを記憶する記憶装置と、

前記カードインタフェースを介してカードに記憶されているＩＤや使用履歴などのカード情報を読み取って前記記憶装置に記憶するとともに、予め決められた手順にもとづいてカード情報を書き換えて、書き換えられたカード情報を前記カードインタフェースを介してカードに書き込むカード情報入出力手段と、

カードのＩＤが前記記憶装置に記憶されているブラックリストに存在するか否かを検索して、もし、存在すれば、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出するＩＤ検索手段と、

前記カードインタフェースを介してカードと通信を行ってカードを認証し、もし、カードが認証されなかったら、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出する認証手段と、

前記通信装置を介してセンタと非リアルタイムで通信して、センタに前記記憶装置に記憶されたカード情報を送信するとともに、センタから前記ブラックリストに追加するＩＤを受信する通信手段とを備えることを特徴とするカード読取書込装置。

【請求項３】　カードの不正な使用を防止するシステムにおいて、

センタ装置と、カードの使用者に対してサービスを提供する外部装置および前記センタ装置に通信可能に接続された複数のカード読取書込装置とを含み、

前記カード読取書込装置は、

前記外部装置との通信を行うための制御信号インタフェースと、

カードとの通信を行うためのカードインタフェースと、

記憶装置と、

前記センタ装置との通信を行うための通信装置と、

前記カードインタフェースを介してカードに記憶されているＩＤや使用履歴などのカード情報を読み取って前記記憶装置に記憶するとともに、予め決められた手順にもとづいてカード情報を書き換えて、書き換えられたカード情報を前記カードインタフェースを介してカードに書き込むカード情報入出力手段と、

カードのＩＤが前記記憶装置に記憶されているブラックリストに存在するか否かを検索して、もし、存在すれば、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出するＩＤ検索手段と、

前記カードインタフェースを介してカードと通信を行ってカードを認証し、もし、カードが認証されなかったら、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出する認証手段と、

前記通信装置を介してセンタと非リアルタイムで通信して、センタに前記記憶装置に記憶されたカード情報を送信するとともに、センタから前記ブラックリストに追加するＩＤを受信する通信手段とを備え、

前記センタ装置は、

前記カード読取書込装置との通信を行うための通信装置と、

記憶装置と、

該記憶装置に記憶されている新しく使われたカードの使用履歴をＩＤ順に並べ替える新履歴ソート手段と、

前記記憶装置に記憶されている過去に使われたカードの使用履歴に、前記新履歴ソート手段でソートされた、新しく使われたカードの使用履歴を追加する新履歴と旧履歴のマージ手段と、

使用履歴が追加されたカードについてカードの使用履歴の推移を評価して、論理的な矛盾が無いか否かを検出し、もし矛盾が検出されたら、そのカードのＩＤを、前記記憶装置に記憶されているマスターブラックリストに登録する矛盾検出手段と、

前記通信装置を介して前記カード読取書込装置と非リアルタイムに通信して、前記カード読取書込装置からカード情報を受信して前記記憶装置に記憶するとともに、前記マスターブラックリストに新たに登録されたＩＤを前記カード読取書込装置に送信する通信手段とを備え、

前記カードは、

前記カード読取書込装置との間の通信を行うためのインタフェースと、

記憶装置と、

該記憶装置に記憶されているＩＤや使用履歴などのカード情報を前記インタフェースを介して前記カード読取書込装置に送信するカード情報送信手段と、
新しいカード情報を前記インタフェースを介して前記カード読取書込装置から受信して前記記憶装置に書き込むカード情報受信手段と、
前記インタフェースを介して前記カード読取書込装置と通信を行ってカードの認証を行う認証手段とを備えることを特徴とする偽造カード使用防止システム。
【請求項４】　前記カード読取書込装置の認証手段は、入力される暗号鍵Ｋにもとづいて、入力されるカードＩＤを暗号化して、暗号文を出力する暗号化手段と、
乱数ｒを生成する乱数生成手段と、
該生成された乱数ｒをカードに送信して、それに対するカードの出力ｘを受信する手段と、
前記暗号化手段から出力された暗号文のうち前記生成された乱数ｒで指定される位置のビット列を選択して出力するセレクタと、
該セレクタの出力とカードの前記出力ｘを比較する比較器とを備え、
前記カードの認証手段は、
予めデータの書き込まれたメモリを備え、前記カード読取書込装置の送信した乱数ｒを前記メモリのアドレスとして、それに対応する前記メモリのデータ出力ｘを前記カード読取書込装置に送信する構成を有することを特徴とする請求項３記載の偽造カード使用防止システム。
【請求項５】　カードとの通信を行うためのカードインタフェースと、該カードインタフェースを介して署名対象カードから読み込んだカードＩＤと別途入力された暗号鍵にもとづいて前記カードＩＤを暗号化する手段とを備え、暗号化によって得られた暗号文を前記カードインタフェースを介して署名対象カードの前記メモリに書き込む構成を有するカード署名装置を備えたことを特徴とする請求項４記載の偽造カード使用防止システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、料金の支払いや身分証明のために用いられるＩＣカードを偽造して不正に使用することを防止する技術に関する。
【０００２】
【従来の技術】我々の身の回りでは、良く知られているように、磁気カードやＩＣカードが、現金や身分証明書の代替として広く使用されている。これらのカードは、しばしば、店員などの人手を介さずに、公衆電話や自動改札機や現金支払機などに投入されて使われる。そのような使われ方がされる用途では、カードの精巧な複製を製造しなくても、カードのデータを別のカードに電子的に複製することで、偽造カードが簡単に製造できるため、偽造カードを製造して不正に利益を得ようとする不心得な者が後を断たない。
【０００３】そこで、クレジットカードでは、センタにカードのＩＤや有効期限や所有者名や使用履歴などのカード情報を登録・照会することが行われていた。なお、ＩＤとは、それぞれのカードに予め割り当てられたカード固有の番号のことである。このようにすれば、偽造カードのＩＤが一旦センタに登録されれば、その偽造カードが使えなくなる。このようなカードの不正な使用を防止する方法としては、例えば特開平３－２５５６８号公報に記載のものがある。
【０００４】また、クレジットカードでは、カード会社しか知らない暗号鍵でＩＤなどのカード情報を暗号化して得られるデータをカードに記録することが行われていた。このようにすれば、カード会社以外の者が新しいＩＤを持つカードを不正に発行することができなくなる。このような防止方法としては、例えば特開平１－２６２８８６号公報や特開昭６２－１８８０７０号公報に記載のものがある。
【０００５】なお、カードの偽造には、正規のカードと同じものを複製するものや、正規のカードのデータを書き換えてカードの価値を大きくするものや（狭義には変造と呼ぶ）、新しいＩＤを持つカードを製造するものがあるが（狭義には偽造と呼ぶ）、以下では特に断りの無い限り、すべてを偽造と呼ぶことにする。
【０００６】また、認証とは、カードと通信することによって、そのカードが正規のものか否かを識別する技術である。暗号とは、暗号鍵に依存して、データ（平文と呼ぶ）を別のデータ（暗号文と呼ぶ）に変換するもので、暗号文から平文が容易に推定できず、また、平文と暗号文から暗号鍵が容易に推定できないような変換のことである。なお、認証や暗号については、例えば、昭晃堂から１９９０年に発行された辻井，笠原編著「暗号と情報セキュリティ」などに詳しい解説がある。
【０００７】
【発明が解決しようとする課題】センタを設置して、カードの使用履歴を問い合わせることで、偽造カードの使用を検出する方法は、クレジットカードならともかく、小額の支払いに用いられるカードシステムには、通信コスト上の問題があるので適用できないという問題があったし、交通料金の支払いに用いられるカードシステムのように短時間で処理しなければならないカードシステムには、センタとの通信に時間がかかるために、適用できないという問題があった。
【０００８】また、カードのＩＤを暗号化して記録する従来の方法では、偽造者がＩＤを自由に選択することは防げるものの、カードを複製して偽造カードを製造することは防げないため、そのような不正な使用を防止することはできなかった。
【０００９】また、認証によってのみカードの不正な使用を防止する方法は、防止効果を高めるために、暗号化のための複雑な処理や多桁整数の四則演算を必要とする

ので、ＩＤカードに搭載されている８ビットのマイクロコンピュータで高速処理することは困難であるという問題があった。

【００１０】本発明は、以上の問題点を解決し、運用コストが小さくて高速に処理できる偽造カード使用防止技術を提供することを目的とする。

【００１１】

【課題を解決するための手段】本発明は、偽造カードの使用を防止する方法において、カード読取書込装置（図１３の１）によってカード（図１３の２）から取得したＩＤや使用履歴などのカード情報を非リアルタイムにセンタ装置（図１３の３）に送信し、センタ装置においてカードの使用履歴の推移を評価して論理的な矛盾を含むカードのＩＤをブラックＩＤとして検出してカード読取書込装置に送信することで、カード読取書込装置の保持するブラックリストを逐次更新し、カードの使用時は、カード読取書込装置において、そのカードのＩＤとブラックリスト中のＩＤとの比較によって不正なカードを検出すると共に、更に、カードとの通信によってそのカードが正規のものか否かを識別する認証を行うことを特徴とする。

【００１２】また、カードの不正な使用を防止する機能を有する本発明のカード読取書込装置は、カードの使用者に対してサービスを提供する外部装置（図１３の４）との通信を行うための制御信号インタフェース（図１の１１０）と、カードとの通信を行うためのカードインタフェース（図１の１４０）と、センタ装置との通信を行うための通信装置（図１の１５０）と、前記センタ装置から送られてきた偽造カードにかかるＩＤを登録してあるブラックリストを記憶する記憶装置（図１の１３０）と、前記カードインタフェースを介してカードに記憶されているＩＤや使用履歴などのカード情報を読み取って前記記憶装置に記憶するとともに、予め決められた手順にもとづいてカード情報を書き換えて、書き換えられたカード情報を前記カードインタフェースを介してカードに書き込むカード情報入出力手段（図１の１２１）と、カードのＩＤが前記記憶装置に記憶されているブラックリストに存在するか否かを検索して、もし、存在すれば、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出するＩＤ検索手段（図１の１２２）と、前記カードインタフェースを介してカードと通信を行ってカードを認証し、もし、カードが認証されなかったら、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出する認証手段（図１の１２３）と、前記通信装置を介してセンタと非リアルタイムで通信して、センタに前記記憶装置に記憶されたカード情報を送信するとともに、センタから前記ブラックリストに追加するＩＤを受信する通信手段（図１の１２４）とを備えることを特徴とする。

【００１３】また、本発明は、偽造カードの使用を防止するシステムにおいて、センタ装置（図１３の３）と、カード（図１３の２）の使用者に対してサービスを提供する外部装置（図１３の４）および前記センタ装置に通信可能に接続された複数のカード読取書込装置（図１３の１）とを含み、前記カード読取書込装置は、前記外部装置との通信を行うための制御信号インタフェース（図１の１１０）と、カードとの通信を行うためのカードインタフェース（図１の１４０）と、記憶装置（図１の１３０）と、前記センタ装置との通信を行うための通信装置（図１の１５０）と、前記カードインタフェースを介してカードに記憶されているＩＤや使用履歴などのカード情報を読み取って前記記憶装置に記憶するとともに、予め決められた手順にもとづいてカード情報を書き換えて、書き換えられたカード情報を前記カードインタフェースを介してカードに書き込むカード情報入出力手段（図１の１２１）と、カードのＩＤが前記記憶装置に記憶されているブラックリストに存在するか否かを検索して、もし、存在すれば、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出するＩＤ検索手段（図１の１２２）と、前記カードインタフェースを介してカードと通信を行ってカードを認証し、もし、カードが認証されなかったら、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出する認証手段（図１の１２３）と、前記通信装置を介してセンタと非リアルタイムで通信して、センタに前記記憶装置に記憶されたカード情報を送信するとともに、センタから前記ブラックリストに追加するＩＤを受信する通信手段（図１の１２４）とを備え、前記センタ装置は、前記カード読取書込装置との通信を行うための通信装置（図６の６５０）と、記憶装置（図６の６３０）と、該記憶装置に記憶されている新しく使われたカードの使用履歴をＩＤ順に並べ替える新履歴ソート手段（図６の６２１）と、前記記憶装置に記憶されている過去に使われたカードの使用履歴に、前記新履歴ソート手段でソートされた、新しく使われたカードの使用履歴を追加する新履歴と旧履歴のマージ手段（図６の６２２）と、使用履歴が追加されたカードについてカードの使用履歴の推移を評価して、論理的な矛盾が無いか否かを検出し、もし矛盾が検出されたら、そのカードのＩＤを、前記記憶装置に記憶されているマスターブラックリストに登録する矛盾検出手段（図６の６２３）と、前記通信装置を介して前記カード読取書込装置と非リアルタイムに通信して、前記カード読取書込装置からカード情報を受信して前記記憶装置に記憶するとともに、前記マスターブラックリストに新たに登録されたＩＤを前記カード読取書込装置に送信する通信手段（図６の６２４）とを備え、前記カードは、前記カード読取書込装置との間の通信を行うためのインタフェース（図４の４１０）と、記憶装置（図４の４３０）と、該

記憶装置に記憶されているＩＤや使用履歴などのカード情報を前記インタフェースを介して前記カード読取書込装置に送信するカード情報送信手段（図４の４２１）と、新しいカード情報を前記インタフェースを介して前記カード読取書込装置から受信して前記記憶装置に書き込むカード情報受信手段（図４の４２２）と、前記インタフェースを介して前記カード読取書込装置と通信を行ってカードの認証を行う認証手段（図４の４２３）とを備えることを特徴とする。

【００１４】また、前記カード読取書込装置の認証手段は、入力される暗号鍵Ｋにもとづいて、入力されるカードＩＤを暗号化して、暗号文を出力する暗号化手段（図１１の１１０２）と、乱数ｒを生成する乱数生成手段（図１１の１１０１）と、該生成された乱数ｒをカードに送信して、それに対するカードの出力ｘを受信する手段（図１１の１１０７，１１０８）と、前記暗号化手段から出力された暗号文のうち前記生成された乱数ｒで指定される位置のビット列を選択して出力するセレクタ（図１１の１１０３）と、該セレクタの出力とカードの前記出力ｘを比較する比較器（図１１の１１０４）とを備え、前記カードの認証手段は、予めデータの書き込まれたメモリ（図１０の１００２）を備え、前記カード読取書込装置の送信した乱数ｒを前記メモリのアドレスとして、それに対応する前記メモリのデータ出力ｘを前記カード読取書込装置に送信する構成を有することを特徴とする。

【００１５】さらに、カードとの通信を行うためのカードインタフェース（図１２の１２０２）と、該カードインタフェースを介して署名対象カードから読み込んだカードＩＤと別途入力された暗号鍵にもとづいて前記カードＩＤを暗号化する手段（図１２の１２０１）とを備え、暗号化によって得られた暗号文を前記カードインタフェースを介して署名対象カードの前記メモリに書き込む構成を有するカード署名装置を備えている。

【００１６】

【作用】従来の偽造カード使用防止技術は、偽造カードの使用が確実に検出できることを目指して設計されていた。しかしながら、偽造カードの使用を確実に検出しようとするからこそ、その不正使用を防止するためのコストが大きくなったり、不正使用の検出に要する時間が長くなると考えられる。そこで、本発明では、発想を転換して、偽造カードの使用を大きな確率で検出できればよしとする。もちろん、クレジット・カードのように、１回あたりの取引額が大きいシステムの場合には、偽造カードの使用者が高額な商品を大量に購入して行方をくらます可能性もあるので、偽造カードの使用を確実に検出しなければならないが、１回あたりの取引額が小さいシステム（市内バスや地下鉄などのプリペイドカードシステム等）の場合には、偽造カードの使用を確実に検出する必要はないのである。なぜなら、１回あたりの取引額が小さい場合には、偽造カードの使用者は、一般に、不正に得られる利益を大きくするために頻繁に偽造カードを使用するので、１回の使用につき或る程度の確率で偽造カードの使用が検出できれば、いつかは偽造カードの使用が検出できるからである。しかも、偽造カードの使用者を拘束できるシステム（例えばカードで交通機関の運賃を支払うようなシステム）においては、偽造カードの使用者から罰金を徴収することによって、偽造カードの使用による過去の損失も補填できるからである。もちろん、偽造カードの使用を確実に検出できないと、少数の使用者が偽造カードを稀に使用している場合には、偽造カードの使用を高い確率で見逃してしまうかもしれない。例えば、悪意を持つ正規の使用者が、プリペイドカードの残高がほとんどゼロになった時に、カードに記録されている残高の額を大きくすれば、そのカードは１回あるいは何回か不正使用されてしまうかもしれない。しかしながら、そのような場合には、偽造カードの使用による損失が極めて小さいので、たとえ検出できなくてもカード・システムの運営者の利益はほとんど損なわれない。なお、偽造カードの使用という不正行為を確率的に見逃してしまうことは、心理的には許容しがたいことかもしれないが、カード・システムの運営者の利益を考慮すると、「不正使用防止のためのコスト」を度外視して「偽造カードの使用による損失」だけを小さくするのではなく、「不正使用防止のためのコスト」と「偽造カードの使用による損失」との合計を小さくすべきなのである。従って、本発明によって「不正使用防止のためのコスト」が大幅に削減できるのであれば、経済的には、そのような見逃しは許容されるであろう。

【００１７】そこで、本発明では、まず、センタを用いる不正使用防止システムにおいて、偽造カードの判定基準を緩くする。すなわち、本発明におけるカード読取書込装置は、カードが入力されるごとにセンタ装置と通信するのではなく、入力されたカードのＩＤがカード読取書込装置の記憶装置に記憶されているブラックリストに登録されているか否かを調べ、もし、ブラックリストにＩＤが存在すれば偽造カードと判定する。また、カード読取書込装置は、カードのＩＤや使用履歴などのカード情報をセンタ装置に送信する。センタ装置への送信は、カード読取書込装置にカードが入力されるごとに行っても良いし、一定時間ごとに行っても良いし、カード情報が一定量だけ蓄積されてから行っても良いし、センタ装置がカード読取書込装置と通信する際に行っても良い。また、通信コストが大きい場合には、カード読取書込装置からセンタ装置へ、すべてのカードのＩＤや使用履歴などのカード情報を送信しないで、一部のカードのＩＤや使用履歴だけを送信しても良い。そして、センタ装置は、カード読取書込装置から送信されるカードのＩＤや使用履歴などのカード情報にもとづいて、偽造カードが使用されたかどうかを判定し、もし偽造カードが存在す

れば、その偽造カードのＩＤを、センタ装置側のマスターブラックリストに登録する。また、センタ装置は、カード読取書込装置と定期的に通信して、前回の通信から現時点までにマスターブラックリストに加わった新しいＩＤをカード読取書込装置に送ってそのブラックリストに登録する。このようにすれば、カード読取書込装置とセンタ装置とがリアルタイムで通信する必要が無くなるので、通信コストも節約できるし、不正使用の判定に要する時間も短く済む。もちろん、以上のようにすると、偽造カードのＩＤがカード読取書込装置側のブラックリストに登録されるまで、その偽造カードの使用を見逃してしまうのだが、カードを１回使用するごとに取り引きされる金額が小さく、ブラックリストの更新時間の間隔が長くなければ、偽造カードによる損害を無視できるほど小さく抑えられる。

【００１８】もっとも、以上のような「センタを用いた不正使用防止方法」は、十分な防止効果を持っていないし、偽造カードが大量に使われると経済的な損失を受けるだけでなくカードシステムを正常に運営すること自体が困難になる。というのも、本発明においては、カード読取書込装置のブラックリストは瞬時に更新されないので、カードの偽造者が、正規のカードとカード読取書込装置の間の通信を盗聴し、盗聴によって得られたカード情報にもとづいて偽造カードを作成して、その偽造カードを使うことが考えられるからである。非接触型のＩＣカードを用いたカードシステムでは、盗聴による偽造は容易である。もちろん、その偽造カードは、ブラックリストが更新されるまでしか、正規のカードとして通用しない。しかしながら、それ故に、カードの偽造者は、多くのＩＤを取得して多数の偽造カードを製造することになる。そして、それらの偽造カードが使われて、それらのＩＤがカード読取書込装置のブラックリストに登録されてしまうと、多数の正規のカードが使えなくなってしまう。カードの偽造者によって悪用されたＩＤが非常に多いと、正規のカードを偽造カードであると判定することが頻繁に発生して、カードシステムの機能が麻痺することも考えられる。以上のような「センタを用いた不正使用防止方法」がこれまで使われなかったのも、おそらく、そのような問題があったからであろう。

【００１９】そこで、本発明では、以上で述べた「センタを用いた不正使用防止方法」に加えて、「認証を用いた不正使用防止方法」を併用することで、偽造カードの使用を検出することにする。認証を併用することは、一見すると、経済性と不正使用防止効果を両立できないように思われる。なぜなら、第１に、現在の認証技術をもってすれば、認証だけでもカードの不正使用を極めて困難にできるので、不正使用防止効果の高い認証方法を用いるのであれば、わざわざセンタを設置する必要なぞないからである。第２に、装置化の容易な簡便な認証方法を採用すれば経済性は損なわれないものの、そのような認証方法には不正使用防止の効果がほとんど無いように思われるからである。しかしながら、本発明においては、カード読取書込装置のブラックリストが更新されるまでの短い期間における偽造カードの使用が、認証によって検出できれば良いのであるし、既に述べたような理由から、偽造カードの使用が大きな確率で検出できれば十分なのであるから、簡便な認証方法を利用できる。

【００２０】

【発明の実施の形態】次に、本発明の実施例について図面を参照して詳細に説明する。

【００２１】図１３は、本発明の偽造カード使用防止システムの一例を示す全体構成図である。この例の偽造カード使用防止システムは、複数のカード読取書込装置１と、これら複数のカード読取書込装置１と有線または無線によって通信可能なセンタ装置３とから構成されている。なお、２はカードを、４はカード２の使用者に対してサービスを提供する外部装置（例えば自動販売機や改札機など）をそれぞれ示す。

【００２２】本例の偽造カード使用防止システムにおいては、各カード読取書込装置１によってカード２から取得したＩＤや使用履歴などのカード情報を非リアルタイムにセンタ装置３に送信し、センタ装置３においてカードの使用履歴の推移を評価して論理的な矛盾を含むカードのＩＤをブラックＩＤとして検出して各カード読取書込装置１に送信することで、各カード読取書込装置１の保持するブラックリストを逐次更新する。なお、カード情報中の使用履歴には、カード使用日時，使用場所を定める情報（例えば各カード読取書込装置に振られた番号など），利用金額などが含まれる。そして、カード２の使用時は、各カード読取書込装置１において、そのカードのＩＤとブラックリスト中のＩＤとの比較によって不正なカードを検出すると共に、更に、カード２との通信によってそのカードが正規のものか否かを識別する認証を行う。偽造カードと判定された場合には外部装置４に制御信号が出され、当該カードを受け付けないようにする処理や警報を発する処理などが外部装置４において行われることにより、偽造カードによる不正な使用を防止する。

【００２３】以下、カード読取書込装置１，カード２およびセンタ装置３の構成例について詳述する。

【００２４】図１は、カード読取書込装置の実施例の基本構成を示す機能ブロック図である。この実施例のカード読取書込装置は、制御信号インタフェース（以下では略して制御信号ＩＦと呼ぶ）１１０と、データ処理装置１２０と、記憶装置１３０と、カードインタフェース（以下では略してカードＩＦと呼ぶ）１４０と、通信装置１５０とから構成されている。

【００２５】制御信号ＩＦ１１０は、自動販売機や改札機などカードの使用者に対してサービスを提供する外部装置とデータ処理装置１２０との間の通信を行うための

回路である。カードＩＦ１４０は、カードとデータ処理装置１２０との間の通信を行うための回路である。記憶装置１３０は、ランダム・アクセス・メモリとリード・オンリ・メモリ（以下ではＲＯＭと呼ぶ）によって構成され、データ処理装置１２０の出力するデータを記憶したり、記憶したデータをデータ処理装置１２０に供給する。通信装置１５０は、センタとデータ処理装置１２０との間の通信を行うための装置である。

【００２６】データ処理装置１２０は、マイクロプロセッサによって構成され、予めＲＯＭに書かれた命令に従って、本カード読取書込装置全体の制御を行う。すなわち、データ処理装置１２０には、カードＩＦ１４０を介してカードに記憶されているＩＤや使用履歴などの情報を読み取って記憶装置１３０に記憶するとともに、必要ならば、自動販売機や改札機などカードの使用者に対してサービスを提供する装置から制御信号ＩＦ１１０を介して供給される料金および現在日時などの情報に基づいて、カード情報の使用履歴などを書き換えて、書き換えられたデータをカードＩＦ１４０を介してカードに書き込むカード情報入出力手段１２１と、カードのＩＤが記憶装置１３０に記憶されているブラックリストに存在するか否かを検索して、もし、存在すれば、カードが偽造カードであることを示すための制御信号を制御信号ＩＦ１１０に送出するＩＤ検索手段１２２と、カードＩＦ１４０を介してカードと通信を行ってカードを認証し、もし、カードが認証されなかったら、カードが偽造カードであることを示すための制御信号を制御信号ＩＦ１１０に送出する認証手段１２３と、通信装置１５０を介してセンタと通信して、センタに対し記憶装置１３０に記憶されたカード情報を送信するとともに、センタからブラックリストに追加するＩＤを受信してブラックリストに追加する通信手段１２４とが、予めＲＯＭに書かれた命令によって、実現されている。

【００２７】図２は、図１のカード読取書込装置の動作のうち偽造カードの検出に関する動作を説明するフローチャートである。図において、カードＩＦ１４０がカードが入力されたことを示す制御信号をデータ処理装置１２０に供給したら、データ処理装置１２０は、まず、カード情報入出力手段１２１によって、カードＩＦ１４０を介してカードに記憶されているＩＤや使用履歴などの情報を読み取って記憶装置１３０に記憶するとともに、必要ならば、自動販売機や改札機などカードの使用者に対してサービスを提供する操作から制御信号ＩＦ１１０を介して供給される料金などの情報にもとづいて、カード情報を書き換えて、書き換えられたデータをカードＩＦ１４０を介してカードに書き込む（２０１）。次に、ＩＤ検索手段１２２によって、当該カードのＩＤが記憶装置１３０に記憶されているブラックリストに存在するか否かを検索して（２０２）、もし、存在すれば、制御を手順２０６に移し、さもなくば、制御を手順２０４に移す（２０３）。

【００２８】手順２０４では、データ処理装置１２０は、認証手段１２３によって、カードＩＦ１４０を介してカードと通信を行ってカードを認証する。そして、もし、カードが認証されなかったら、制御を手順２０６に移し、さもなくば、処理を終了する（２０５）。他方、手順２０６においては、データ処理装置１２０は、カードが偽造カードであることを示すための制御信号を制御信号ＩＦ１１０に送出して、処理を終了する。

【００２９】図３は、図１のカード読取書込装置の動作のうちセンタとの通信に関する動作を説明するフローチャートである。図において、通信装置１５０がセンタからの通信が入ったことを示す制御信号をデータ処理装置１２０に供給したら、データ処理装置１２０は、通信手段１２４によって、通信装置１５０を介してセンタと通信して、記憶装置１３０に記憶されていたカード情報をセンタに送信して（３０１）、記憶装置１３０に記憶されていた上記カード情報を消去する（３０２）。次に、センタからブラックリストに追加するＩＤを受信し（３０３）、この受信したＩＤを記憶装置１３０に記憶されているブラックリストに登録して（３０４）、処理を終了する。

【００３０】図４は、カードの実施例の基本構成を示す機能ブロック図である。この実施例のカードは、インタフェース（以下では略してＩＦと呼ぶ）４１０と、データ処理装置４２０と、記憶装置４３０とから構成されている。

【００３１】ＩＦ４１０は、当該カードとカード読取書込装置との間の通信を行うための回路である。記憶装置４３０は、ランダム・アクセス・メモリとＲＯＭによって構成され、データ処理装置４２０の出力するデータを記憶したり、記憶したデータをデータ処理装置４２０に供給する。

【００３２】データ処理装置４２０は、マイクロプロセッサによって構成され、予めＲＯＭに書かれた命令に従って、当該カードの制御を行う。すなわち、データ処理装置４２０には、記憶装置４３０に記憶されているＩＤや使用履歴などの情報をＩＦ４１０を介してカード読取書込装置に送信するカード情報送信手段４２１と、新しいカード情報をＩＦ４１０を介してカード読取書込装置から受信して記憶装置４３０に書き込むカード情報受信手段４２２と、ＩＦ４１０を介してカード読取書込装置と通信を行ってカードの認証を行う認証手段４２３とが、予めＲＯＭに書かれた命令によって、実現されている。なお、認証については後で詳しく述べるが、本実施例における認証手段４２３は、複雑な処理を必要としないので、データ処理装置４２０を、処理能力の低い８ビットのマイクロプロセッサで実現できる。

【００３３】図５は、図４のカードの動作を説明するフローチャートである。図において、ＩＦ４１０を介して

カード読取書込装置から通信を要求する制御信号がデータ処理装置４２０に供給されたら、データ処理措置４２０は、カード情報送信手段４２１によって、記憶装置４３０に記憶されているＩＤや使用履歴などの情報をＩＦ４１０を介してカード読取書込装置に送信し（５０１）、次に、カード情報受信手段４２２によって、新しいカード情報をＩＦ４１０を介してカード読取書込装置から受信して記憶装置４３０に書き込む（５０２）。次に、認証手段４２３によって、ＩＦ４１０を介してカード読取書込装置と通信を行ってカードの認証を行い（５０３）、処理を終了する。なお、認証方法については後で詳しく述べるが、手順５０３における認証は、カード読取書込装置における図２の手順２０４における認証と対応するもので、同じ手順ではない。

【００３４】図６は、センタ装置の実施例の基本構成を示す機能ブロック図である。この実施例のセンタ装置は、データ処理装置６２０と、記憶装置６３０と、通信装置６５０とから構成されている。

【００３５】記憶装置６３０は、ランダム・アクセス・メモリやＲＯＭによって構成され、データ処理装置６２０の出力するデータを記憶したり、記憶したデータをデータ処理装置６２０に供給する。通信装置６５０は、データ処理装置６２０とカード読取書込装置との間の通信を行うための装置である。

【００３６】データ処理装置６２０は、マイクロプロセッサによって構成され、予めＲＯＭに書かれた命令に従って、当該センタ装置の制御を行う。すなわち、データ処理装置６２０には、記憶装置６３０に記憶されている新しく使われたカードの使用履歴をＩＤ順に並べかえる新履歴ソート手段６２１と、記憶装置６３０に記憶されている過去に使われたカードの使用履歴に、新しく使われたカードの使用履歴を追加する、新履歴と旧履歴のマージ手段６２２と、使用履歴が追加されたカードについてカードの使用履歴の推移を評価して、論理的な矛盾が無いか否かを検出し、もし矛盾が検出されたら、そのカードのＩＤを、記憶装置６３０に記憶されているマスターブラックリストに登録する矛盾検出手段６２３と、通信装置６５０を介してカード読取書込装置と通信して、カード読取書込装置からカード情報を受信して記憶装置６３０に記憶するとともに、マスターブラックリストに新たに登録されたＩＤ（ブラックＩＤ）をカード読取書込装置に送信する通信手段６２４とが、予めＲＯＭに書かれた命令によって、実現されている。

【００３７】図７は、図６のセンタ装置の動作のうち偽造カードの検出に関する動作を説明するフローチャートである。図において、データ処理装置６２０は、まず、新履歴ソート手段６２１によって、記憶装置６３０に記憶されている新しく使われたカードの使用履歴をＩＤ順に並べかえる（７０１）。次に、新履歴と旧履歴のマージ手段６２２によって、記憶装置６３０に記憶されている過去に使われたカードの使用履歴に、新しく使われたカードの使用履歴を追加する（７０２）。次に、矛盾検出手段６２３によって、使用履歴が追加されたカードで手順７０３の処理がまだ行われていないカードについて、使用履歴の推移を評価して、論理的な矛盾が無いか否かを検出し（７０３）、もし矛盾が検出されたら、制御を手順７０５に移し、さもなくば制御を手順７０６に移す（７０４）。論理的な矛盾としては、例えば、同じＩＤのカードがほぼ同時刻に別々の場所（別々のカード読取書込装置）で使用されているといったことがあげられる。

【００３８】次に、手順７０５では、矛盾の検出されたカードのＩＤを、記憶装置６３０に記憶されているマスターブラックリストに登録し（７０５）、制御を手順７０６に移す。手順７０６では、使用履歴が追加されたすべてのカードについて手順７０３が実行されたか否かを調べ、もし、使用履歴が追加されたすべてのカードについて手順７０３が実行済みであれば、処理を終了し、さもなくば、制御を７０３に移す。

【００３９】図８は、図６のセンタ装置の動作のうちカード読取書込装置との間の通信に関する動作を説明するフローチャートである。図において、データ処理装置６２０は、まず、通信手段６２４によって、通信装置６５０を介して、カード読取書込装置との通信を開始し（８０１）、次に、カード読取書込装置から新しく使われたカードのカード情報を受信し（８０２）、次に、マスターブラックリストに新たに登録されたブラックＩＤをカード読取書込装置に送信し（８０３）、すべてのカード読取書込装置との交信が実行されたか否かを調べ、もし、すべてのカード読取書込装置との交信が実行済みであれば、処理を終了し、さもなくば、新しいカード読取書込装置を選択して、制御を８０１に移す（８０４）。

【００４０】次に、カード読取書込装置とカードとの間において行われる認証について説明する。

【００４１】図９は、図１のカード読取書込装置の認証手段１２３および図４のカードの認証手段４２３において用いられている認証方法を説明するシーケンスチャートである。図において、まず、カード読取書込装置が乱数ｒを生成して（９０１）、乱数ｒをカードｉに送信する（９０２）。なお、ここで、ｉはこのカードのＩＤとする。そして、カードｉは、カード読取書込装置から乱数ｒを受信し（９０２）、乱数ｒを関数S_iに入力して得られる出力ｘを求め（９０３）、ｘをカード読取書込装置に送信する（９０４）。カード読取書込装置は、ｘを受信して（９０４）、乱数ｒを関数S_iに入力して得られる出力とｘとを比較し（９０５）、もし、等しければ、通信相手のカードは正規のカードであると判定し、さもなくば、通信相手のカードは偽造カードであると判定する。なお、関数S_iはカードｉに固有な関数で、カードｉは、関数S_iだけを持っており、カード読取書込

装置は、すべてのｉについて、カードｉの関数S_iを持っている。

【００４２】図１０は、図４のカードの認証手段４２３の構成例を示す機能ブロック図である。本発明においては、カードが１回使用されるごとに確実にではなく或る程度の確率で偽造カードが検出できれば良いから、関数S_iの入出力ビット数を小さくできる。図の実施例では、関数S_iは、カード読取書込装置から送信された８ビットの乱数ｒを入力端子１００１を介して関数S_i１００２に入力して、出力端子１００３に出力される８ビットの出力ｘをカード読取書込装置に送信している。なお、関数S_iの入出力ビット数が僅か８ビットなので、関数S_i１００２は、僅か２５６バイトの（１バイトは８ビットとする）ＲＯＭ（１回書き込み可能なＲＯＭ）で構築できる。つまり、ＲＯＭ中に２５６バイトの関数S_iを保持し、８ビットの乱数ｒをアドレスとして、それに対応するＲＯＭの８ビットの出力をｘとする。

【００４３】図１１は、図１のカード読取書込装置における認証手段１２３の構成例を示す機能ブロック図である。図において、暗号関数１１０２は、入力端子１１０６から供給される暗号鍵Ｋにもとづいて、入力端子１１０５から入力されるカードＩＤ（以下ではｉとする）に対して暗号化を施して、得られた長さ２５６バイトの暗号文（後述するように正規のカードの場合は、この暗号文がカード署名装置によってカードｉの上記ＲＯＭに書き込まれている）を、セレクタ１１０３に供給する。乱数発生器１１０１は、８ビットの乱数ｒを発生して、乱数ｒを出力端子１１０７を介してカードに送信するとともに、セレクタ１１０３にも供給する。セレクタ１１０３は、乱数ｒに依存して、暗号関数１１０２の出力する２５６バイトのうち１バイトを選択して、選択されたバイトを比較器１１０４に供給する。比較器１１０４のもう一方の入力には、カードから送信されたｘが入力端子１１０８を介して供給されている。そして、比較器１１０４は、セレクタ１１０３の出力とｘとを比較して、比較結果を出力端子１１０９から出力する。比較器１１０４が一致を検出した場合、当該カードは正規のカードあると判定される。以上のようにして、カード読取書込装置における認証手段１２３を実現すれば、カード読取書込装置にすべてのカードのＲＯＭの内容（関数S_iの内容）を記憶する必要が無い。

【００４４】図１２は、カードのＲＯＭに関数S_i（図１０の１００２）を書き込むためのカード署名装置の実施例を示す機能ブロック図である。図において、予めカードＩＤの書き込まれているカードが、カードインタフェース（以下ではカードＩＦと呼ぶ）１２０２に差し込まれると、カードＩＦ１２０２を介して、カードＩＤが読み込まれて、読み込まれたカードＩＤが暗号関数１２０１に供給される。暗号関数１２０１は、図１１の暗号関数１１０２と等価な暗号装置で、入力端子１２０３から供給される暗号鍵Ｋ（図１１の入力端子１１０６に加わる暗号鍵Ｋと等価）にもとづいて、カードＩＤに暗号化を施して、得られた２５６バイトの暗号文を、カードＩＦ１２０２を介して、カードの関数S_i（図１０の１００２）を構成しているＲＯＭに書き込まれる。

【００４５】なお、以上の実施例においては、カードの関数S_i（図１０の１００２）を構成しているＲＯＭとして、１回書き込み可能なＲＯＭを用いたが、書き込んだ内容を保存できるものであれば、どのようなメモリを用いてもよい。また、以上の実施例においては、暗号関数の構成方法については述べなかったが、暗号関数の構成方法は、本発明と直接関係ないので、任意の暗号関数が使える。秘密鍵暗号を用いても良いし、必要ならば、公開鍵暗号を用いても良いし、フィードバック・シフトレジスタを用いても良い。なお、暗号関数をフィードバック・シフトレジスタで構成する場合には、例えば、フィードバック・シフトレジスタの係数を暗号鍵として、フィードバック・シフトレジスタの初期状態をカードＩＤとし、暗号文をフィードバック・シフトレジスタの出力とすれば良い。また、以上の実施例においては、暗号関数に供給する暗号鍵Ｋを固定として考えていたが、暗号鍵Ｋを定期的に変更しても良い。

【００４６】また、以上の実施例においては、使用されたすべてのカードのカード情報をセンタ装置に送信していたが、偽造される危険性が少ない用途においては、選択された一部のカードのカード情報だけを送信することにより、センタ装置に送信する情報を削減することも可能である。例えば、カードＩＤのハッシュ値が予め定められた値をとるものについてだけ、カード情報を送信するのである。これは、すなわち、カード全体を検査するのではなく、一部のカードだけを抜き打ち検査するということである。一人の偽造者が、多数のＩＤを利用して、偽造カードを製造している場合には、この方法でも、偽造カードを効果的に検出できる。

【００４７】

【発明の効果】第１の効果は、通信コストが小さく済むということである。なぜなら、センタを用いる従来の不正使用防止システムにおいては、端末からセンタに、すべてのカードのＩＤと使用履歴をリアルタイムで送信し、そのカードが正規のものかどうかの判定結果をセンタから受信しなければならなかったが、本発明においては、センタ装置のマスターブラックリストの移しを各カード読取書込装置が保持しており、ブラックリストによる偽造カードの検出に際して、センタ装置とリアルタイムで送信する必要がないからである。また、必要に応じて、一部のカードのＩＤと使用履歴だけを送信することで、送信するデータの量を削減できるからである。

【００４８】第２の効果は、装置コストが小さくて済むということである。なぜなら、本発明は、ブラックリストによる偽造カードの検出を補完するためにカードの認

証を導入しており、認証手段は簡便なもので済むため、カードとカード読取書込装置との通信や認証において、複雑な暗号方式を使う必要が無いからである。もっとも、本発明は、カードの認証を行わなければならないので、磁気カードには適用できない。すなわち、本発明は、ＩＣカードを用いたカードシステムにしか適用できない。しかしながら、本発明は、他のカードシステムと違い、認証暗号回路の搭載されている専用の高価なＩＣカードを使わなくとも、８ビットのマイクロプロセッサしか搭載されていない汎用の安価なＩＣカードでも、高い不正使用防止効果が発揮できるので、ＩＣカードのコストが低下している今日においては、コストの問題はほとんど無視できる。特に、非接触型のＩＣカードを使用した交通料金を支払うようなシステムにおいては、多くの場合、マイクロプロセッサや通信のための回路が搭載されているので、コストの問題はほとんど無視できる。

【００４９】第３の効果は、高速に処理できるということである。なぜなら、既に述べたように、処理時間のかかる複雑な暗号方式を使う必要もないし、センタ装置とリアルタイムで通信する必要も無いからである。

【００５０】第４の効果は、偽造カードの検出能力が高いということである。なぜなら、本発明のカード不正使用防止技術を無効にして、偽造カードを使用する方法は、以下で述べるように、原理的にはいくつか考えられるが、いずれの方法も、実際に実行することは難しいからである。第１の攻撃方法としては、偽造カードの使用者が、予め複数のカードの複製を作成しておき、それらを時間に応じて使い分けることが考えられる。もし、偽造カードの使用者のすべてが決められた時間に決められた偽造カードを使用し、一旦使用した偽造カードを２度と使わないようにすれば、カードの運営者が偽造カードの使用を検出してそのカードのＩＤをブラックリストに加えても、偽造カードの使用は防止できない。しかしながら、偽造カードの製造者は正規のカードを大量に調達しなければならないので、偽造カードの製造者が利益を得ることは難しい。また、仮に、偽造カードを大量生産して販売したとしても、カードの販売が発覚する危険が高くなるし、使用者の不注意や偽造カードを使用する時間のミスなどで、決められた時間に決められた偽造カードが使われないことが高い確率で生じ、多くの偽造カードの多くが使えなくなる。従って、ブラックリストが更新される時間の間隔が適切であれば、この攻撃方法は有効ではない。第２の攻撃方法は、大量の偽造カードを使用して、マスターブラックリストやブラックリストをオーバーフローさせて、偽造カード使用防止方法の運用を妨害する方法である。しかしながら、今日では大容量の記憶装置が安価に入手できるし、マスターブラックリストやブラックリストはＩＤだけのリストであるから、偽造カードの数を上回る膨大な数のＩＤを容易に記憶できる。従って、カード読取書込装置およびセンタ装置の記憶装置の記憶容量が適切に選択されていれば、そのような攻撃を実行するのは困難である。

【図面の簡単な説明】

【図１】カード読取書込装置の実施例の基本構成を示す機能ブロック図である。

【図２】カード読取書込装置の動作のうち偽造カードの検出に関する動作を説明するフローチャートである。

【図３】カード読取書込装置の動作のうちセンタとの通信に関する動作を説明するフローチャートである。

【図４】カードの実施例の基本構成を示す機能ブロック図である。

【図５】カードの動作を説明するフローチャートである。

【図６】センタ装置の実施例の基本構成を示す機能ブロック図である。

【図７】センタ装置の動作のうち偽造カードの検出に関する動作を説明するフローチャートである。

【図８】センタ装置の動作のうちカード読取書込装置との間の通信に関する動作を説明するフローチャートである。

【図９】カード読取書込装置の認証手段およびカードの認証手段において用いられている認証方法を説明するシーケンスチャートである。

【図１０】カードの認証手段の構成例を示す機能ブロック図である。

【図１１】カード読取書込装置における認証手段の構成例を示す機能ブロック図である。

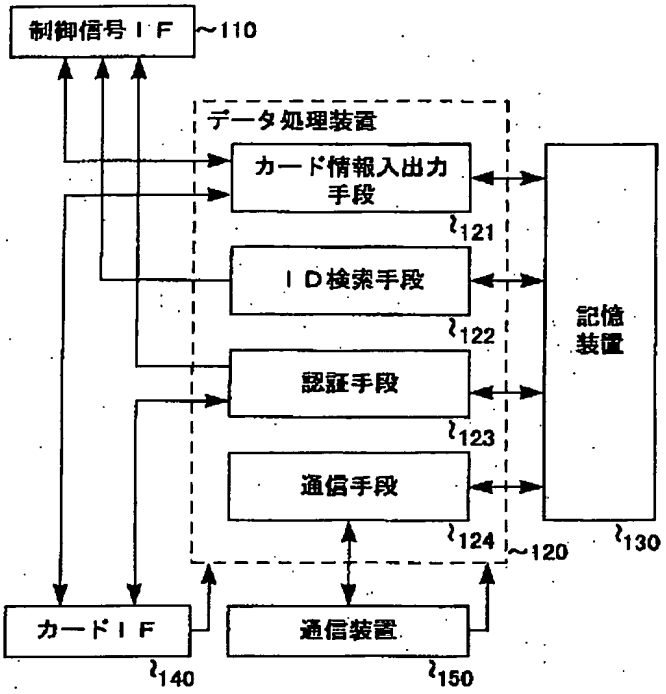
【図１２】カード署名装置の実施例を示す機能ブロック図である。

【図１３】本発明の偽造カード使用防止システムの一例を示す全体構成図である。

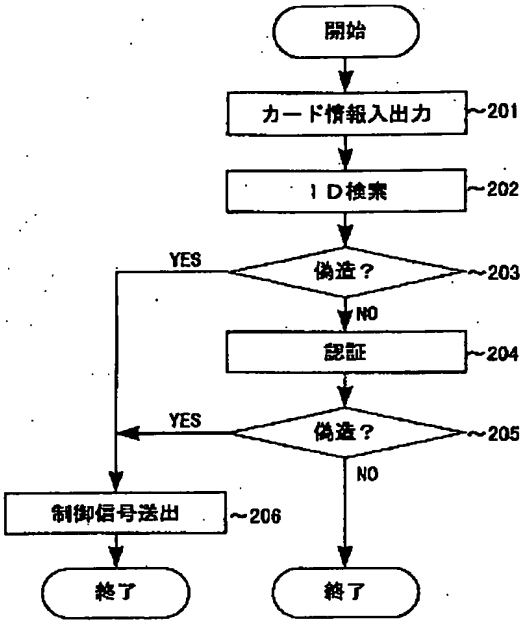
【符号の説明】

１…カード読取書込装置
２…カード
３…センタ装置
４…外部装置
１１０…制御信号インタフェース
１２０，４２０，６２０…データ処理装置
１３０，４３０，６３０…記憶装置
１４０，１２０２…カードインタフェース
１５０，６５０…通信装置
４１０…インタフェース
１００２…関数S_i
１１０１…乱数発生器
１１０２，１２０１…暗号関数
１１０３…セレクタ
１１０４…比較器

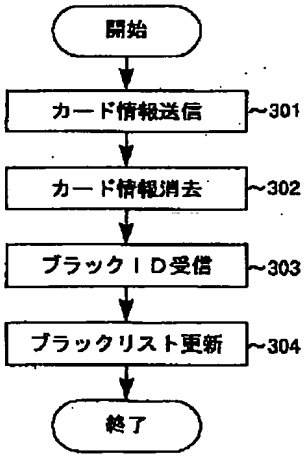
【図１】


制御信号ＩＦ
110
データ処理装置
カード情報入出力手段
121
ＩＤ検索手段
122
認証手段
123
通信手段
124
120
記憶装置
130
カードＩＦ
140
通信装置
150

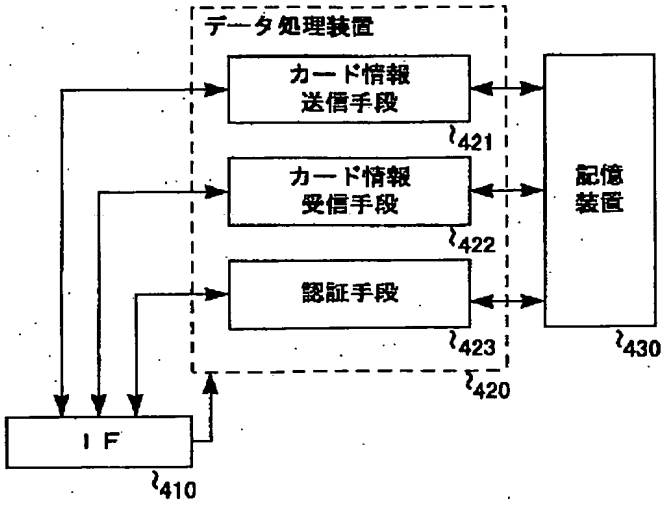
【図２】


開始
カード情報入出力
201
ＩＤ検索
202
YES
偽造？
203
NO
認証
204
YES
偽造？
205
NO
制御信号送出
206
終了
終了

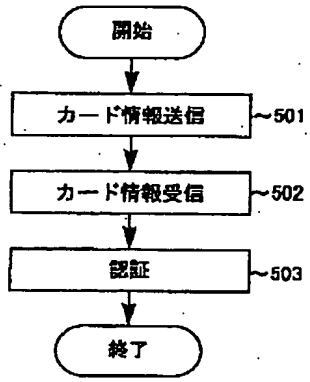
【図３】


開始
カード情報送信
301
カード情報消去
302
ブラックＩＤ受信
303
ブラックリスト更新
304
終了

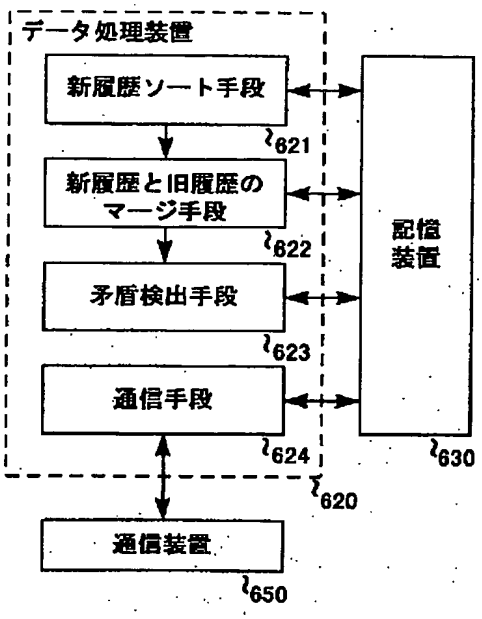
【図４】


データ処理装置
カード情報送信手段
421
カード情報受信手段
422
認証手段
423
420
記憶装置
430
ＩＦ
410

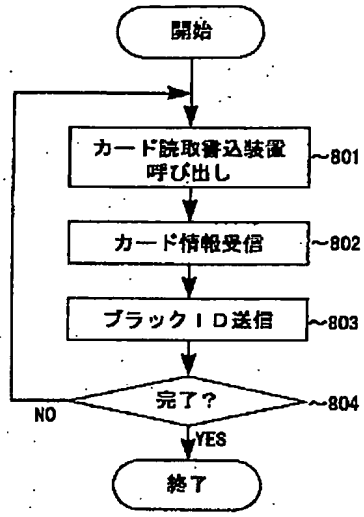
【図５】



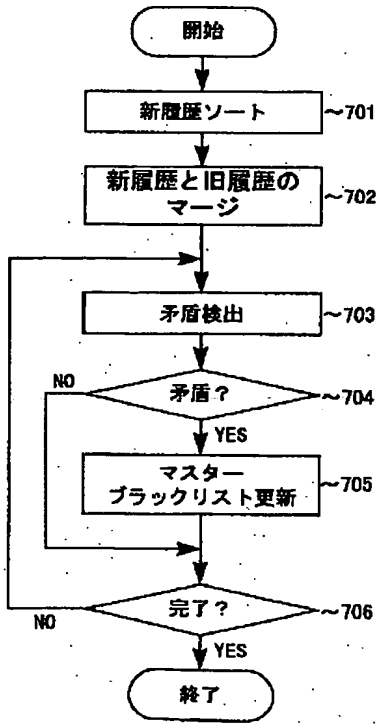
【図６】



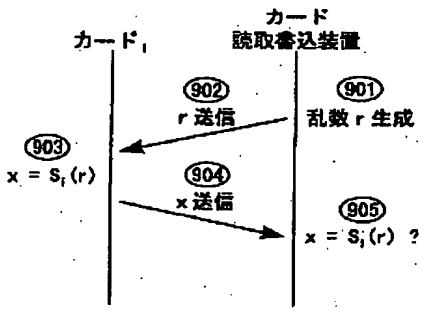
【図８】



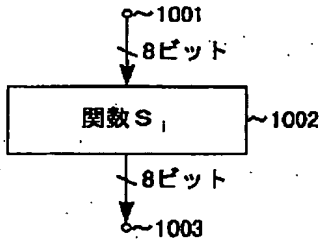
【図７】



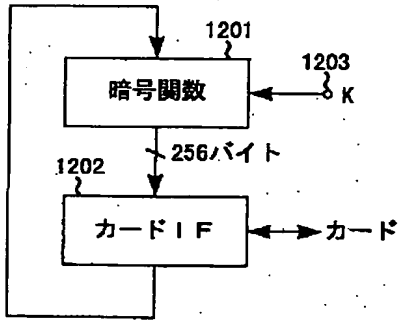
【図９】



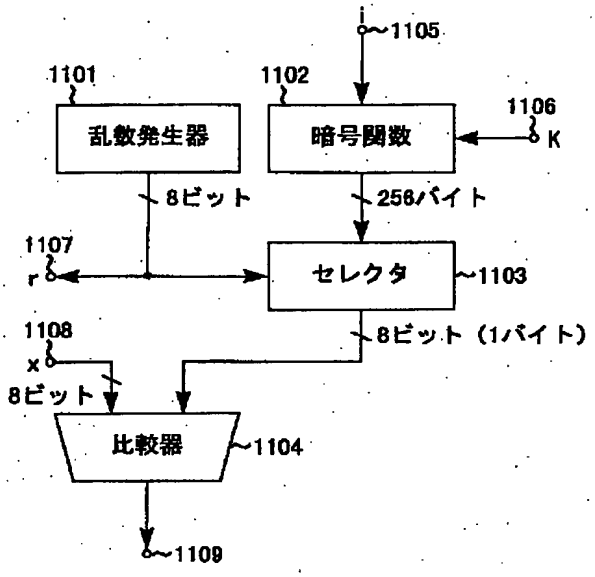
【図１０】



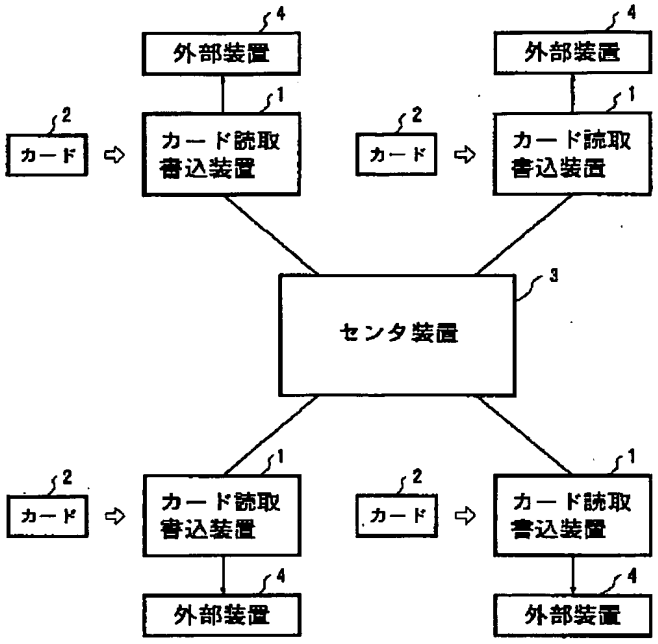
【図１２】



【図１１】


1105
1101
1102
乱数発生器
暗号関数
1106
K
8ビット
256バイト
1107
r
セレクタ
1103
8ビット（1バイト）
1108
x
8ビット
比較器
1104
1109

【図１３】


4
外部装置
1
2
カード
カード読取
書込装置
センタ装置
3